Individuals Internet Security Perceptions and Behaviors: Polycontextual Contrast between Ghana and Nigeria.

Alfred Paa Gyaisey & Richard Boateng
Department of Information Systems
University of Ghana
Legon, Accra, Ghana
E-mail: paagyaisey@gmail.com; richard.boateng@gmail.com

ABSTRACT

Security is one of the most important aspect of life needed to ensure continuation from one generation to the next regardless of the specie. As human crave security in their daily lives, security over the internet is one that has become necessary over the past decade or two. This study envisaged to examine the internet security perceptions of Ghanaian and Nigerian internet users and how these perceptions affect their behaviors. This study draws on two important theories *(a) contextualization of the Protection Motivation Theory [PMT]* and *(2) a polycontextual lens for cross-national comparisons of internet security behaviors among Ghanaians and Nigerians*. A qualitative research approach was devised through focus group discussions to collect data by examining various themes. Study was made up of thirty respondents (fifteen each) from both countries. It was evidently established that internet security perceptions affect internet users' behaviors.

Keywords: Internet Security, Perceptions, Behaviors, Polycontextual Contrast, Ghana and Nigeria.

iSTEAMS Cross-Border Conference Proceedings Paper Citation Format
Mary Julius Egbai & Chukwueloka S. Uduagwu (2018): Individuals Internet Security Perceptions and Behaviors: Polycontextual Contrast Between Ghana And Nigeria.. Proceedings of the 13th iSTEAMS Multidisciplinary Conference, University of Ghana, Legon, Accra, Ghana. Vol. 2, Pp 115-118

1. INTRODUCTION

The behavioral aspect of security in both work and personal settings has recently drawn attention from IS researchers due to the dramatic increase in Internet users worldwide, the pervasive use of the Internet in all aspects of life, and the fact that individual users "represent a significant point of weakness in achieving the security of the cyber infrastructure" (Anderson and Agarwal 2010).

Research Problem

On the African continent, studies on internet and cybersecurity and actions to curtail cybercrime are quite limited, in the context of Ghana, it is virtually nonexistent. As the use of internet of the continent grows on a daily basis, it is important to understand how online security issues are affecting internet user's behaviors. Thus, there is a gap in our knowledge about the range of users' online security coping behaviors. Further, this lack of focus on understanding internet user's behaviors from different context on the African continent, affects policy direction of the African Union, ECOWAS etc. The problem of how internet security perceptions are affecting internet users behaviors and within different context is highly critical for informing directions and measures and therefore needs to be addressed.

Research Purpose

Having established the gap in knowledge on internet security perceptions on the African continent and it associated behaviors, this study sought to examine the behaviors of internet users in two different context based on their perception of internet security. This study also sought to understand the strategies that these internet users have adopted in coping with these security threats that they encounter when using the internet. This study had the purpose of understanding these behaviors in the Ghanaian and the Nigerian context which was important to give a broader perspective, increasing the scope and generalizability of the study, in understanding the themes of the study.

RESEARCH QUESTION

By establishing the research problem and the purpose for the study, the following questions served as a guide for the study

b) What is the state of internet security in Africa?
c) What is the security perception of internet users within the Ghanaian and Nigerian context?
d) What are the coping strategies that internet users in these two countries are adopting in their use of the internet?

2. RESEARCH METHODOLOGY

This study adopted a qualitative approach in understanding the various themes. Specifically, this study was designed as an inductive exploration. Due to a lack of empirical evidence on the subject matter, an exploratory tool was important to understand the various themes under consideration. A scale was developed by adopting aspects Chen and Zehadi (2016) themes in accessing the internet security perception and behaviors of Americans against Chinese. This scale was redesigned to fit the Ghanaian and Nigerian context. The scale consisted of four major themes: Perceived Security Threat, Self-Efficacy, Susceptibility, Action.

A sample of thirty respondents were used and out of which five groups of three were formed. Based on the interview guide that was developed, interview sessions were held for various groups of participants from each country. Each interview session lasted for approximately more 30 minutes. Nigerians based in Ghana were interviewed for this study. In order to ensure a good contextual fit of the response from the Nigerians, the interview guide was redesigned into an open ended questionnaire and was mailed to Nigerian research team member who administered it to Nigerian respondents based in Nigeria.

3. FINDINGS

Findings were discussed based on the themes

- **Perceived Security Threat**

In all, there was a general perception of security threat among both Ghanaian and Nigerian respondents. Respondents confessed that they felt a high degree of exposure based on personal experience and those of friends. They also expressed great worry and very anxious due to the possibility of losing personal data due to internet security attacks.

- **Self-Efficacy**

Self-Efficacy was defined as a respondent's ability to deal with internet security attacks based on how resourced they are in terms knowledge, available support, tools, etc. This theme was measured with three basic questions: whether they had adequate knowledge to deal with threat of security, whether it is difficult for them to get appropriate advice and whether it is difficult to get such advice. Over two-third of respondents, both Ghanaians and Nigerians, confessed of not being in the position to deal with online security threats.

- **Susceptibility**

This theme examined respondents feeling of susceptible to internet security attacks. All respondents confessed of being susceptible to internet security attacks. Over half of respondents shared personal experience or experience of close relatives/friends who have had some form of attacks such as hacking, phishing, etc.

- **Action**

The Action theme enquired from respondents what active measures they have taken or putting in place to control or counter any form of internet security attacks. Simply, respondents were asked two basic questions: if there was any action at all against internet security attacks and secondly, if there is any plan in place against internet security attacks. Some respondents claimed to have taken some action such as signing out or logging out whenever they logged on to their online accounts. Some respondents also asserted to given false information especially when they deem the request of the online platform too personal.

4. IMPLICATIONS

Theoretical Implications

Using the Collectivist and Individualist dichotomy of cultural differentiation, both Ghana and Nigeria fall within the collectivist sect of cultural practice. It is noteworthy that such cultural sect believes in the corporate gain and lose of its members, hence a member's concern is one that is shared among all members of the sect and there is a high degree of confidence and trust among member's intentions and ability to render help (Bandura, 2015). However, even within such collectivist cultures, there is an expression of difference in their collectivism with some instance positing a display of individualism (Chen and Zehadi, 2016). Evidence from this study indicate that although these two countries practice collectivism, there was low level of trust from perspective of respondents in seeking help from experts in dealing with possible internet security threat. This trust is rather displayed among the smaller circus of friends who may not necessarily be experts on issue at hand. In suing the Protection Motivation Theory (PMT) and the Technology Threat Acceptance Theory (TTAT) as a guide, respondents from this study showed that, as they feel the need to protect themselves from the possible security threat, they are also ready to take up steps in coping with these threats by adopting Action plans such as always logging out after using the internet, providing minimal personal information or not signing up to platform at all.

Practical/Policy Implications

On a national level, the only major thing that seem to be happening in terms of internet or cyberspace security is that of legislation across the continent (African Union Convention On Cyber Security and Personal Data Protection, 2014; Cyber Security in Tanzania – Country Report, 2005; Tanzania Cyber Security Report, 2016; Balcha Reba, 2005)
With Western countries spending billions of dollars in fighting cybercrime and internet security, countries in Africa need to go beyond legislation and put in more resources. It is such lack of confidence which demonstrated itself among respondents who were not even ready to seek help from experts.

5. ORIGINALITY

An original research paper is based on original research that produces new knowledge instead of summarizing what is already known in a new form. There are many ways to produce new knowledge such as through observations, experiments, new approaches to solving existing problems, etc. Very often, an original research work is simply called a dissertation.
This study is considered original based on the following

- It is the report of a study written by the researchers who actually did the study
- The researchers described the research question and the purpose of the study
- The research detail their research method
- The results of the research are reported
- The researcher interprets their results and discuss possible implications

REFERENCE

1. Anderson, C. L., & Argawal, R. (2010). PRACTICING SAFE COMPUTING: A MULTIMETHOD EMPIRICAL EXAMINATION OF HOME COMPUTER USER SECURITY BEHAVIORAL INTENTIONS . *Management Information Systems Quarterly*.
2. Boudreau, M.-C., Gefen, D., & Straub, D. W. (2001). *Validation in Information Systems Research: A State-of-the-Art Assessment.* Minesota: Management Information Systems Research Centre.
3. Caudill, E. M., & Murphy, P. E. (2000). Consumer Online Privacy: Legal and Ethical Issues. *Journal of Public Policy and Marketing*, pp. 7-19.
4. Chen, Y., & Zahedi, M. (2016). INDIVIDUALS' INTERNET SECURITY PERCEPTIONS AND BEHAVIORS: POLYCONTEXTUAL CONTRASTS BETWEEN THE UNITED STATES AND CHINA. *Management Information Systems Quarterly.*, 205-222.
5. Culnan, M. J., & Armstrong, P. K. (1999). *Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical.* INFORMS.
6. Goodman, S. E., & Lin, H. S. (2001). *Toward a Safer and More Secure Cyberspace.* Washington: National Academies Press.
7. Hamamura, T., Meijer, Z., & Heine, S. (2009). Approach-Avoidance Motivation and Information Processing: A Cross-Cultural Analysis. *Personality and Socail Psychology Bulletin*.
8. Johston, A. C., & Warkentin, M. (2010). *Fear Appeals and Information Security Behaviors: An Empirical Study.* Minesota: Management Information Systems Research Centre.
9. Liang, H., & Xue, Y. (2009). *Avoidance of Information Technology Threats: A Theoretical Perspective.* Minesota: MIS Quarterly.
10. Lloyd, J. (2000). *Cyber Security in Tanzania-Country Report.* Information Technology Law.
11. Mbarawa, M. M. (May, 2016.). *National Information and Communications Technology Policy.* Tanzania: Ministry of Works, Transport and Communication.
12. Parliament of Mauritius, O. (2003). *Computer Misuse and Cybercrime Act 2003.* Parliamnet of Mauritius.
13. Parliamnet of South Africa, O. (2002). *Electronic Communications and Transactions Act.* South Africa: Parliamnet of South Africa.
14. Reba, B. (June, 2005). *State of Cyber Secuirty in Ethiopia.* Ethiopian Telecommunications Agency.
15. Serianu, O. (2016). *Tanzania Cyber Security Report.* Serianu.
16. WISR, O. (2007). *World Information Society Report.* World Information Society.
17. WSIS. (Tunis, 16-18 November 2005). *Report of the Tunis phase of the World Summit on the Information Society, .* Geneva: World Summit of Information Society.